IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of:	Nelson Waldo Bunker V, David Laizerovich, Eva Elizabeth Bunker and Joey Don Van Schuyver
Serial No.:	10/043,654
Confirmation No.:	7438
Filed:	January 10, 2002
Group:	2134
Examiner:	Tongoc Tran
For:	NETWORK SECURITY TESTING

Mail Stop Appeal
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

This Brief is submitted in connection with an appeal from the final rejection of the Examiner, dated July 11, 2006, finally rejecting claims 1, 2, 4, 6-8, 10-14, 16, 18-21, 23, 25, 26, 28, 30-35, 58, 62-64, 68-70, 74-76, 80-84, 86-90 and 103-105, all of the pending claims in this application.

REAL PARTY IN INTEREST

The real party in interest is ACHILLES GUARD, INC. d/b/a CRITICAL WATCH., a United States Company having a principal office and place of business at 6060 N. Central Expressway, Suite 560, Dallas, Texas 75206.

RELATED APPEALS AND INTERFERENCES

There are no related appeals and no related interferences regarding the above-identified patent application.

STATUS OF CLAIMS

Claims 1, 2, 4, 6-8, 10-14, 16, 18-21, 23, 25, 26, 28, 33-35, 58, 62-64, 68-70, 74-76, 80-84, 86-90 and 103-105 are pending, stand finally rejected, and are on appeal here. Claims 1, 2, 4, 6-8, 10-14, 16, 18-21, 23, 25, 26, 28, 33-35, 58, 62-64, 68-70, 74-76, 80-84, 86-90 and 103-105 are set forth in the CLAIMS APPENDIX attached hereto.

STATUS OF AMENDMENTS

No amendments were entered in response to the Final Office Action dated July 11, 2006. The claims attached in the Appendix of this Appeal Brief are Claims 1, 2, 4, 6-8, 10-14, 16, 18-21, 23, 25, 26, 28, 33-35, 58, 62-64, 68-70, 74-76, 80-84, 86-90 and 103-105 as presently pending.

SUMMARY OF CLAIMED SUBJECT MATTER

Claim 1 is directed to a network security testing apparatus. The apparatus includes a first tester for testing network security vulnerabilities of a network system under test and is adapted to communicably couple to a network system under test. (Fig. 5, Paragraph 108) The first tester is adapted to perform a plurality of sequential tests on the system under test to obtain network security vulnerability information. The sequential tests return network security vulnerability information relating to the network system under test. The network security vulnerability information provided by each of the plurality of sequential tests is more specific to the network system under test than the network's security vulnerability information provided by a previous test. Each of the sequential tests are more specifically configured to adapt to the security obstacles of the system under test based upon the information gained from the previous test and

the test further obtain additional network security vulnerability information from the network system under test (paragraph [0076] to paragraph [0078]).

Claim 13 is directed to a network security testing method. The method involves executing a first test by a first tester in order to test for network security vulnerabilities of a network system under test. The first test is targeted at the network system under test and the tester is communicably coupled to the network system under test. Information is received execution of the first test. The first information consists of the network security vulnerability information. A second test is executed to test for the network vulnerabilities of the network system under test after receiving the first information. The second test is more specifically configured to adapt to security obstacles of the network system under test based upon information gained from the first test and to obtain second information from the network system under test based upon the first information. The second information comprises additional network security vulnerability information that is more specific to the network system under test than the first information. Next, second information is received responsive to the second test after execution of the second test. This process may be completed until desired information of a system under test has been achieved. Each time the test is performed, the network security vulnerability information attained from a subsequent test is more specific to the system under test based upon the network security vulnerability information provided by each previous test (paragraphs [0076] - [0078]).

Claim 25 is directed to a computer program for network security testing stored on a computer readable medium. The program includes instructions for performing the method described in Claim 13 (paragraphs [0076] - [0078]).

Claim 58 is directed to a network security testing apparatus that includes a plurality of testers for testing network security vulnerabilities of a network system under test to obtain network security vulnerability information. The plurality of testers is each adapted to communicably couple to a network system under test. Tests are performed on the network system under test by a selected tester (Figure 5). The selection of the tester adapts to detected security obstacles in the network system under test based upon information gained from a

previous test to obtain more specific network security vulnerability information from the network system under test (paragraphs [0076] - [0078]). Said testers have load balance characteristics describing a degree of balance of the loads of testers of said plurality of testers and the selected tester is selected from said plurality of testers based upon optimizing the load balance characteristic.

Claim 64 comprises a network security testing method involving selecting a tester from a plurality of testers that test for network security vulnerabilities of a network system under test to obtain network security vulnerability information (Figure 5). The selection of said tester is to adapt to security obstacles of the network system under test detected based upon information gained from a previous test to obtain more specific network security vulnerability information from the network system under test. The method then executes a test by the selected tester wherein the test is targeted at the network system under test and wherein the selected tester is communicably coupled to the network system under test (paragraphs [0076] - [0078]). The plurality of testers has a load balance characteristic describing a degree of balance of loads of testers of the plurality of testers and the selection of a selected tester from a plurality of testers is based at least partially on optimizing the load balance characteristics.

Claim 70 relates to a computer program for network security testing stored in a computer readable medium. The computer program comprises instructions for performing the method described previously with respect to claim 64 (paragraphs [0076] - [0078]).

Claim 76 comprises a network security testing apparatus comprising a first tester that is adapted to communicably couple to a network system under test to perform network security vulnerability testing. The first tester is adapted to perform a test on the network system under test to obtain network security vulnerability information (Figure 5). The first tester is further adapted to make a first attempt to communicably couple to the network system under test before executing the test to obtain network security vulnerability information. The first tester is also adapted to make a second attempt to communicably couple to the system under test after executing the test to obtain network security vulnerability information and the combination of a

success of the first attempt and the failure of a second attempt are interpreted as the detection of the test by the network system under test (paragraphs [0128] - [0129]).

Claim 80 describes a network security testing method including the steps of attempting the first communication by a first tester and executing a test to obtain network security vulnerability information by the first tester. The method further includes the steps of attempting a second communicable coupling by the first tester to the network security system under test after executing the test to obtain network security vulnerability information and then interpreting the combination of a success of the first communicably coupling and the failure of the second communicable coupling as detection of the test by the network security system under test (paragraphs [0128] - [0129]).

Claim 84 comprises a computer program for network security testing stored on a computer readable medium. The program includes instructions for performing the method described with respect to claim 80 (paragraphs [0128] - [0129]).

Claim 88 comprises a network security testing apparatus including a tester that is communicably coupled to a system under test for testing for network security vulnerabilities. A test tool within the tester performs a test to obtain specific network security vulnerability information of the network system under test (Figure 5). The test tool is selectable responsive to adapt to the security obstacles of the network system under test based on information gained from previously received network security vulnerability information (paragraphs [0076] – [0078]). An application program interface is adapted to interface between said tester and said test tool. Said application program interfaces further includes an API stub enabling said test tools to be executed by said tester even if the outputs of said tester do not directly correspond to the inputs of said test tool. The test tool may be executed by said tester even if the inputs of the tester do not directly correspond to the outputs of said test tool. The application program interface further includes a common API for interfacing between the test tool and instructions provided to the test tool. The tester is adapted to test the system under test by execution of the test tool (paragraph [0132]).

Claim 89 comprises a network security testing method including the steps of adapting an application program interface to interface between a tester and a test tool. The test tool may be executed by the tester even if the outputs of the tester do not directly correspond to the inputs of the test tool and the test tool may be executed by the tester even if the inputs of the tester do not directly correspond to the outputs of the test tool. The method further comprises the step of executing the test tool by the tester and the test tool is targeted at a system under test and the tester is communicably coupled to the system under test (paragraphs [0132] – [0138]).

Claim 90 comprises a computer program for network security testing stored on a computer readable storage medium. The computer program includes instructions for performing the method described with respect to claim 89 (paragraphs [0132] - [0138]).

Claim 103 describes a network security testing apparatus including a plurality of testers wherein each of the plurality of testers is adapted to communicably couple to a system under test (Figure 5). Each tester of the plurality of testers has at least one quality of communicable coupling to the system under test. The at least one quality of communicable coupling including cost per bit, absolute speed and geographical proximity of the selected tester to the system under test (paragraph [0196]). A test of the system under test is performed by a selected tester of the plurality of testers, a selected tester being selected from a plurality of testers based on at least partially the customer profile (paragraph [0201]). The selected tester is selected from the plurality of testers based at least partially on the selected tester's quality of communicable coupling.

Claim 104 is directed to a method for network security testing including the step of selecting a tester from a plurality of testers based at least partially on a tester's quality of communicable coupling. Quality of communicable coupling includes at least one of cost per bit, absolute speed and geographical proximity of the selected tester to the system under test (paragraph [0196]). The method further includes the step of executing a test by the selected tester, wherein the test is targeted at a system under test and wherein the selected tester is communicably coupled to the system under test (Figure 5).

Claim 105 comprises a computer program for network security testing stored on a computer readable medium. The program includes instructions for performing the method described with respect to step 104.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Are Claims 1, 2, 4-6, 10-14, 16, 18-21, 23, 25, 26, 28 and 33-35 novel over the *Gleichauf* reference? Are Claims 58, 62-64, 68-70 and 74-75 of the Applicant's invention rendered obvious by the combined teachings of *Gleichauf* and the *Li, et al* references, are Claims 80-84, 86 and 87 rendered obvious by the combined teachings of *Gleichauf* in view of *Polk*, are Claims 88-90 rendered obvious by the combined teachings of *Gleichauf* and S*rinivasan*, and are Claims 103-105 rendered obvious by *Gleichauf* in view of *Gleichauf* '668?

It is believed that Claims 1, 2, 4-6, 10-14, 16, 18-21, 23, 25, 26, 28, 33-35, 58, 62-64, 68-70 and 74-75 stand or fall together as Group 1, Claims 76, 80-84, 86 and 87 stand or fall together as Group 2, Claims 88-90 stand or fall together as Group 3, and Claims 103-105 stand or fall together as Group 4.

ARGUMENT

The Claims present in this application stand rejected under both 35 U.S.C. § 102 and 35 U.S.C. § 103(a). Accordingly, the issues remaining in this Appeal are the novelty of Applicants' invention over the *Gleichauf* reference and the obviousness of Applicants' invention over the *Gleichauf* reference in combination with various prior art. Applicants respectfully submit that the invention, as claimed, would be novel over the *Gleichauf* reference and that the invention, as claimed, would not be obvious to one of ordinary skill in the art based upon a fair reading of the references cited. Furthermore, as will be set forth below, it is unclear how one of ordinary skill in the art would have been motivated to combine the references in the manner set forth in the final rejection, or what, if any, motivation has been shown to exist for one of ordinary skill in the art to combine the references.

Claim 1 recites the limitations of (emphasis added):

> wherein each of the plurality of sequential tests are adapted to return the network security vulnerability information regarding the network system under test, the network security vulnerability information provided by each of the plurality of sequential tests being more specific to the network under test than the network security vulnerability information provided by a previous test;
>
> wherein each of the plurality of sequential tests are more specifically configured to adapt to the security obstacles of the network system under tests detected based on information gained from the previous tests and obtain additional network security vulnerability information from the network system under test.

The recitations from the *Gleichauf* reference do not describe a network security testing apparatus operating in this fashion. *Gleichauf* describes a system wherein a first group of tests are run to assess the system and obtain vulnerability information. These tests within the group of tests do not progressively improve with each test to adapt to the security obstacles of the network, but instead are run with no consideration given to the results of previously received test results within the group of tests. After the initial vulnerability assessment phase is completed, an active exploit phase is performed wherein vulnerabilities detected by the first group of tests are exploited by the system described in *Gleichauf*. This is significantly different from the limitations described with respect to Applicants' Claim 1. In Applicants' Claim 1, each of the plurality of sequential tests are more specifically configured to adapt to the security obstacles of the network system under test based upon the results of a previous test. A first group of tests does not have to first be completed. *Gleichauf* describes a second group of tests based upon the result of a first group of tests, but does not describe each test adapted to security obstacles based upon a previous test, only a second group based upon a first group.

Thus, Applicants' Claim 1 describes a system that improves its testing process each time new test results are received. *Gleichauf* does not improve its testing methodology in this manner. *Gleichauf* describes a system that obtains a number of system vulnerabilities based upon a first group of tests, and then using these detected vulnerabilities, runs a next group of tests to exploit the detected vulnerabilities. The system is not progressively improving as each

set of test results are received by the system. Furthermore, the network security vulnerability information provided by each of the plurality of tests is more specific to the network system under test than the network security vulnerability information provided by a previous test. Thus, the information provided by the tests run in Applicants' Claim 1 becomes progressively more specific to the network under test with each successive test. This type of successive improvement of the information obtained from each test result is not described by the *Gleichauf* reference. For these reasons, Claim 1, and all claims dependent therefrom, are allowable over the recited art.

Claims 13, 25, 58, 64 and 70 are independent claims including limitations similar to those described with respect to Claim 1. Applicants respectfully submit that Claims 13, 25 58, 64, and 70, and all claims dependent therefrom, are allowable over the recited reference for similar reasons to those described with respect to Claim 1.

Claims 76, 80-84, 86 and 87 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Gleichauf, et al* in view of *Polk*. Claim 76 describes the operation of the Applicants' system within a network security vulnerability testing scheme. The *Polk* reference describes the classification of tests as passive or active, and the transformation of an active test into a network worm does not illustrate the limitations described in Applicants' Claim 76, 80, and 84. The Final Office Action dated July 11, 2006, admits that *Gleichauf* does not explicitly disclose wherein said first tester is adapted to make a second attempt to communicably couple to the system under test after the test; and wherein the combination of success of the first attempt and the failure of the second attempt are interpreted as the detection of the test by the system under test. The official action of July 11, 2006, describes the *Polk* reference as disclosing active and passive tests and the transformation of active tests into a Trojan horse or network worm. However, it does not seem that the disclosure in *Polk* of passive and active tests and the transformation of active tests into a Trojan horse or network worm comprise a disclosure of a first tester adapted to make a second attempt to communicably couple to the system under test after a first test wherein the combination of the success of the first test and the failure of the second test being interpreted as detection of the tests by the system under test. The recognition of passive and active tests and the conversion of active tests into a worm do not describe these

limitations. Thus, we believe that Claims 76, 80, and 84 are allowable over the recited *Gleichauf* and *Polk* references.

Claims 88-90 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Gleichauf* in view of *Srinivasan*. Claim 88 includes the limitation of:

> a test tool within the tester for performing a test to obtain specific network security vulnerability information for the network system under test, said test tools selectable responsive to adapt to the security obstacles of the network system under test detected based on information gained from a previously received information on network security vulnerability information;

The *Gleichauf* reference, as described previously with respect to Claim 1, does not describe a selection of test tools to adapt to the security obstacles of the network system under test based upon information gained from previously received information on network security vulnerability information. The *Gleichauf* reference describes the performance of a first phase of tests that detect vulnerabilities and then the performance of a second phase of tests that exploit these vulnerabilities. The selection of a test tool responsive to a detected security obstacle is not described by the recited references. Therefore, Applicants respectfully submit that Claim 88 is distinguishable from the combination of the *Gleichauf* and *Srinivasan* references. Claims 89 to 90 are allowable for similar reasons.

Claims 103-105 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Gleichauf* in view of *Gleichauf* '668. Claim 103 includes the limitation of a plurality of testers "wherein each tester of said plurality of testers has at least one quality of communicable coupling to the system under test, be at least one quality of communicable coupling including costs per bit, absolute speed, and geographical proximity of the selected tester to the system under test." Each of these limitations of costs per bit, absolute speed and geographical proximity are not described within either of the *Gleichauf* references. Furthermore, the official action of July 11, 2006, does not discuss all of these limitations. Claim 104 and 105 include similar limitations. Therefore, the Applicants respectfully submit that Claims 103 through 105 are allowable over the recited art since the prior art fails to show each limitation of the claims.

MPEP §2142 specifies that:

> The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

In regard to what an examiner must show in order to establish a prima facie case of obviousness, MPEP §2142 further explains that:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. . . . Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

In regard to what an examiner must do in order to meet the first criterion for a prima facie rejection, MPEP §2143.01 specifies that:

> Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art.

In the present situation, as explained in more detail below, the various combinations of references proposed by the Examiner are not supported by a proper suggestion or motivation to

make each proposed modification. This means that the first criterion for a prima facie rejection has not been met, which in turn means the Examiner has failed to carry the burden of establishing a prima facie rejection. In addition, certain claim limitations are not taught or suggested by the cited combinations, which means that the third criterion for a prima facie rejection has not been met and that the Examiner has failed to carry the burden of establishing a prima facie rejection for this independent reason.

As stated by the Federal Circuit in *Cardiac Pacemakers, Inc. v. Guidant Sales Corp.*, 381 F.3d 1371, 1376 (Fed. Cir. 2004), "[w]hen prior art references require selective combination by the court to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight gleaned from the invention itself." Moreover, the Federal Circuit has recently stated that "[a]s this court outlined in *Ruiz v. A.B. Chance Co., 357 F.3d 1270, 1275 (Fed. Cir. 2004)*, in making the assessment of differences between the prior art and the claimed subject matter, *section 103* specifically requires consideration of the claimed invention 'as a whole.' Inventions typically are new combinations of existing principles or features.... The "as a whole" instruction in title 35 prevents evaluation of the invention part by part. *Ruiz, 357 F.3d at 1275*. Without this important requirement, an obviousness assessment might successfully break an invention into its component parts, then find a prior art reference corresponding to each component. Id. This line of reasoning would import hindsight into the obviousness determination by using the invention as a roadmap to find its prior art components. Further, this improper method would discount the value of combining various existing features or principles in a new way to achieve a new result-often the essence of invention. Id." *Princeton Biochemicals, Inc. v. Beckman Coulter, Inc.*, 411 F.3d 1332, 1337 (Fed. Cir. 2005).

Applicant submits that the official action has taken the approach specifically forbidden by the Federal Circuit in *Princeton Biochemicals* and has simply broken Applicant's invention into its component parts, and then attempted to find a prior art reference corresponding to each component. As such, Applicant submits that support for the combination is based on hindsight and the combination is therefore improper.

The official action with respect to Claim 58, 62, 64, 68, 70 and 74 recited "*Gleichauf* does not teach the plurality of testers has a load balance characteristic describing a degree of balance of loads of testers wherein the selected tester is selected from a plurality of testers based at least partially on optimizing the load balance characteristics. However, *Li, et al* teaches using distributing parallel processing on heterogeneous networks of workstations as effective load sharing of works resource (*Li*, third paragraph, page 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement *Gleichauf*'s teaching of accessing network vulnerability with *Li*'s teaching of implementing parallel processing to balance network workloads for sharing CPU and memory resources."

The official action dated July 11, 2006, has provided no indication of a suggestion within either the *Gleichauf* or *Li* references for combining those references in the manner suggested. It merely states that the teachings would be combined to balance the network loads for sharing CPU and memory resources. However, there is no discussion that the *Gleichauf* reference suggests a need for balancing network loads within its network vulnerability testing operations nor does it suggest that there may be a need for the sharing of CPU and memory resources. Furthermore, the *Li* reference while describing load sharing of resources does not provide any suggestion that this type of implementation may be effective in network vulnerability testing. Therefore, Applicants' submit that the official action has taken the approach specifically forbidden by the Federal Circuit in *Princeton Biochemicals* and has simply broken Applicants' invention into its component parts, and then attempted to find prior art references corresponding to each component. As such, Applicants submit that support for the combination is based on hindsight and the combination is therefore improper.

Furthermore, with respect to Claims 76, 80-84, 86 and 87, the official action dated July 11, 2006, recites "*Gleichauf* does not explicitly disclose wherein said first tester is adapted to make a second attempt to communicably couple to the system under test after the test; and wherein the combination of the success of the first attempt and failure of second attempt are interpreted as detection of the tests by the system under test. However, *Polk* discloses tests for system vulnerability may mimic an attacker or simply browse through the system in a more typical auditing fashion. . .therefore it would have been obvious to one of ordinary skill in the art

at the time the invention was made to incorporate the teaching of *Gleichauf*'s tester placed outside of the internal network for a better view of the system with *Polk*'s teaching of customized protective testing measure to ensure the system may not transform into a network work after the active testing is completed."

Applicants respectfully submit that the recited reasons for combination are not suggested within either of the references. Nothing in *Gleichauf* suggests that placing a tester outside of the network provides a better view of the system that would ensure the ability to prevent active tests from transforming into a network worm. While the *Gleichauf* reference describes a system capable of detecting network vulnerabilities, nothing in *Gleichauf* suggests that it is useful for detecting or preventing the transformation of active tests into network worms. Therefore, Applicants respectfully submit that in addition to failing to describe the disclosed limitations of Applicants' claims as described previously hereinabove, the official action has attempted to merely break Applicants' invention into its component parts and recite prior art references corresponding to these parts without providing sufficient support for the combination of the references other than hindsight based upon the Applicants' disclosure.

Respectfully submitted,
HOWISON & ARNOTT, L.L.P.
Attorneys for Applicants

/Brian D. Walker Reg. #37751/
Brian D. Walker
Registration No. 37751

BDW/ljo

CLAIMS APPENDIX

1. (Previously Presented) A network security testing apparatus comprising:

a first tester for testing for network security vulnerabilities of a network system under test that is adapted to communicably couple to a the network system under test, said first tester adapted to sequentially perform a plurality of sequential tests on the system under test to obtain network security vulnerability information;

wherein each of the plurality of sequential tests are adapted to return the network security vulnerability information regarding the network system under test, the network security vulnerability information provided by each of the plurality of sequential tests being more specific to the network system under test than the network security vulnerability information provided by a previous test;

wherein each of the plurality of sequential tests are more specifically configured to adapt to the security obstacles of the network system under test detected based on information gained from the previous test and obtain additional network security vulnerability information from the network system under test.

2. (Previously Presented) The network security testing apparatus of claim 1, wherein each of the plurality of sequential tests are more specifically configured to adapt to system configuration of the network system under test based on the information gained from the previous test and obtain the additional network security vulnerability information from the network system under test.

3. (Canceled)

4. (Previously Presented) The network security testing apparatus of claim 3 1, wherein the network security vulnerability information includes information regarding network connectivity from the first tester to the network system under test.

5. (Canceled)

6. (Previously Presented) The network security testing apparatus of claim1, wherein the network security vulnerability information includes connection information relating to an IP address used in the previous test.

7. (Previously Presented) The network security testing apparatus of claim 3 1, further comprising:

a second tester that is adapted to communicably couple to the network system under test;

wherein the previous test is executed by said first tester;

wherein determination of whether a subsequent test is executed by said first tester or by said second tester is made based at least partially upon the network security vulnerability information obtained by the previous test in order to adapt to the security obstacles of the network under test.

8. (Previously Presented) The network security testing apparatus of claim 7, wherein the subsequent test includes execution of a test tool selected from a plurality of test tools based at least partially upon the network security vulnerability information obtained by the previous test.

9. (Canceled)

10. (Previously Presented) The network security testing apparatus of Claim 1, wherein the plurality of tests continue until all relevant information about the system under test has been collected.

11. (Previously Presented) The network security testing apparatus of claim 7, wherein the subsequent test includes execution of a test tool selected from a plurality of test tools based at least partially upon the system environment information.

12. (Canceled)

13. (Previously Presented) A network security testing method comprising:

a) executing a first test by a first tester to test for network security vulnerabilities of a network system under test, wherein the first test is targeted at a network system under test, and wherein the first tester is communicably coupled to the network system under test;

b) receiving first information from the first test about the system under test, after executing the first test, the first information comprising network security vulnerability information;

c) executing a second test to test for the network vulnerabilities of the network system under test after said receiving first information, wherein the second test is more specifically configured to adapt to the security obstacles of the network system under test detected based on information gained from the first test and obtain second information from the network system under test based on the first information, the second information comprising additional network security vulnerability information more specific to the network system under test than the first information;

d) receiving the second information from the second test about the network system under test, after executing the second test;

e) repeating steps a)-d) a plurality of times until relevant information about the system under test has been collected; and

f) wherein the network security vulnerability information obtained from each subsequent test is more specific to the system under test based on the network security vulnerability information provided by each previous test.

14. (Original) The network security testing method of claim 13, wherein the time period between said executing the first test and said executing the second test can be negligible.

15. (Canceled)

16. (Previously Presented) The network security testing method of claim 13, wherein said network security vulnerability information comprises information regarding network connectivity from the first tester to the network system under test.

17. (Canceled)

18 (Previously Presented) The network security testing method of claim 17, wherein said receiving network security vulnerability information comprises receiving connection information relating to an IP address used in said executing the first test.

19. (Previously Presented) The network security testing method of claim 13, further comprising determining whether the second test will be executed by the first tester or by a second tester based upon the network security vulnerability information from the first test, before said executing the second test.

20. (Previously Presented) The network security testing method of claim 13, further comprising selecting the second test from a plurality of tests based at least partially upon the network security vulnerability information.

21. (Previously Presented) The network security testing method of claim 13, further comprising:

determining whether all possible network security vulnerability information regarding the system under test has been received in light of the plurality of tests; and

executing additional tests until all possible network security vulnerability information regarding the system under test has been received in light of the plurality of tests.

22. (Canceled)

23. (Previously Presented) The network security testing method of claim 19, further comprising selecting the second test from a plurality of tests based at least partially upon the network security vulnerability information.

24. (Canceled)

25. (Previously Presented) A computer program product for network security testing stored in a computer-readable medium, comprising:

a) instructions for executing a first test by a first tester to test for network security vulnerabilities of a network system under test, wherein the first test is targeted at a network system under test, and wherein the first tester is communicably coupled to the network system under test;

b) instructions for receiving first information from the first test about the system under test, after executing the first test, the first information comprising network security vulnerability information;

c) instructions for executing a second test to test for the network security vulnerabilities of the network system under test after said receiving first information, wherein the second test is more specifically configured to adapt to the security obstacles of the network system under test detected based on information gained from the first test and obtain second information from to the network system under test based on the first information, the second information comprising additional network security vulnerability information more specific to the network system under test than the first information;

d) instructions for receiving the second information from the second test about the network system under test, after executing the second test;

e) instructions for repeating steps a)-d) a plurality of times until all relevant information about the system under test has been collected; and

f) instructions for wherein the network security vulnerability information obtained from each subsequent test is more specific to the system under test based on the network security vulnerability information provided by each previous test.

26. (Original) The computer program product of claim 25, wherein the time period between executing the first test and executing the second test can be negligible.

27. (Canceled)

28. (Previously Presented) The computer program product of claim 25, wherein said network security vulnerability information comprises information regarding network connectivity from the first tester to the network system under test.

29. (Canceled)

30. (Previously Presented) The computer program product of claim 25, wherein receiving network security vulnerability information comprises receiving session establishability information relating to an IP address used in executing the first test.

31. (Previously Presented) The computer program product of claim 25, further comprising instructions for determining whether the second test will be executed by the first tester or by a second tester based upon the network security vulnerability information from the first test, before said executing the second test.

32. (Previously Presented) The computer program product of claim 25, further comprising instructions for selecting the second test from a plurality of tests based at least partially upon the network security vulnerability information.

33. (Previously Presented) The computer program product of claim 25, further comprising:

instructions for determining whether all possible network security vulnerability information regarding the system under test has been received in light of the plurality of tests; and

instructions for executing additional tests until all possible network security vulnerability information regarding the system under test has been received in light of the plurality of tests.

34. (Canceled)

35. (Previously Presented) The computer program product of claim 31, further comprising instructions for selecting the second test from a plurality of tests based at least partially upon the network security vulnerability information.

36. (Canceled)

37. (Canceled)

38. (Canceled)

39. (Canceled)

40. (Canceled)

41. (Canceled)

42. (Canceled)

43. (Canceled)

44. (Canceled)

45. (Canceled)

46. (Canceled)

47. (Canceled)

48. (Canceled)

49. (Canceled)

50. (Canceled)

51. (Canceled)

52. (Canceled)

53. (Canceled)

54. (Canceled)

55. (Canceled)

56. (Canceled)

57. (Canceled)

58. (Previously Presented) A network security testing apparatus comprising:

a plurality of testers for testing for network security vulnerabilities of a network system under test to obtain network security vulnerability information;

wherein each of said plurality of testers is adapted to communicably couple to a network system under test;

wherein a test of the network system under test is performed by a selected tester of said plurality of testers, said selection of said selected tester to adapt to detected security obstacles of the network system under test based on information gained from a previous test to obtain more specific network security vulnerability information from the network system under test;

wherein said plurality of testers has a load balance characteristic describing a degree of balance of loads of testers of said plurality of testers; and

wherein the selected tester is selected from said plurality of testers based additionally on optimizing the load balance characteristic.

59. (Canceled)

60. (Canceled)

61. (Canceled)

62. (Original) The network security testing apparatus of claim 58,

wherein each tester of said plurality of testers has at least one quality of communicable coupling to the system under test; and

wherein the selected tester is selected from said plurality of testers based at least partially on the selected tester's quality of communicable coupling.

63. (Original) The network security testing apparatus of claim 62, wherein the quality of communicable coupling includes:

cost per bit;

absolute speed; and

geographical proximity of the selected tester to the system under test.

64. (Previously Presented) A network security testing method comprising:

selecting a selected tester from a plurality of testers for testing for network security vulnerabilities of a network system under test to obtain network security vulnerability information, said selection of said selected tester to adapt to security obstacles of the network system under test detected based on information gained from a previous test to obtain more specific network security vulnerability information from network system under test;

executing a test by the selected tester, wherein the test is targeted at a the network system under test, and wherein the selected tester is communicably coupled to the network system under test;

wherein the plurality of testers has a load balance characteristic describing a degree of balance of loads of testers of the plurality of testers; and

wherein said selecting a selected tester from a plurality of testers is further based at least partially on optimizing the load balance characteristic.

65. (Canceled)

66. (Canceled)

67. (Canceled)

68. (Previously Presented) The network security testing method of claim 64,

wherein each tester of the plurality of testers has at least one quality of communicable coupling to the network system under test; and

wherein said selecting a selected tester from a plurality of testers is further based at least partially on the selected tester's quality of communicable coupling.

69. (Previously Presented) The network security testing method of claim 68, wherein the quality of communicable coupling includes:

cost per bit;

absolute speed; and

geographical proximity of the selected tester to the system under test.

70. (Previously Presented) A computer program product for network security testing stored in a computer-readable medium, comprising:

instructions for selecting a selected tester from a plurality of testers for testing for network security vulnerabilities of a network system under test to obtain network security vulnerability information, said selection of said selected tester to adapt to security obstacles of the network system under test detected based on information gained from a previous test to obtain more specific network security vulnerability information from network system under test;

instructions for executing a test by the selected tester, wherein the test is targeted at a system tinder test, and wherein the selected tester is communicably coupled to the network system under test;

wherein the plurality of testers has a load balance characteristic describing a degree of balance of loads of testers of the plurality of testers; and

wherein the selecting a selected tester from a plurality of testers is further based at least partially on optimizing the load balance characteristic.

71. (Canceled)

72. (Canceled)

73. (Canceled)

74. (Previously Presented) The computer program product of claim 70,

wherein each tester of the plurality of testers has at least one quality of communicable coupling to the system under test; and

wherein the selecting a selected tester from a plurality of testers is further based at least partially on the selected tester's quality of communicable coupling.

75. (Previously Presented) The computer program product of claim 74, wherein the quality of communicable coupling includes:

cost per bit;

absolute speed; and

geographical proximity of the selected tester to the system under test.

76. (Previously Presented) A network security testing apparatus comprising:

a first tester that is adapted to communicably couple to a network system under test to perform network security vulnerability testing, wherein said first tester is adapted to perform a test on the network system under test to obtain network security vulnerability information on the network system under test;

wherein said first tester is adapted to make a first attempt to communicably couple to the network system under test before executing the test to obtain network security vulnerability information;

wherein said first tester is adapted to make a second attempt to communicably couple to the system under test after executing the test to obtain network security vulnerability information ; and

wherein the combination of success of the first attempt and failure of the second attempt are interpreted as detection of the test by the network system under test.

77. (Canceled)

78. (Canceled)

79. (Canceled)

80. (Previously Presented) A network security testing method comprising:

attempting a first communicable coupling by a first tester for performing network security vulnerability testing to a network system under test;

executing a test to obtain network security vulnerability information by the first tester, wherein the test is targeted at the network system under test;

attempting a second communicable coupling by the first tester to the network system under test after executing the test to obtain network security vulnerability information; and

interpreting the combination success of the first communicable coupling and failure of the second communicable coupling as detection of the test by the network system under test.

81. (Original) The network security testing method of claim 80, further comprising receiving security obstacle information of the system under test, responsively to said executing the test.

82. (Original) The network security testing method of claim 80, further comprising:

attempting a third communicable coupling to the system under test;

wherein said attempting a first communicable coupling is made using a first originating IP address;

wherein said attempting a second communicable coupling is made using a second originating IP address that is essentially the same as the first originating IP address;

wherein said attempting a third communicable coupling is made using a third originating IP address that is different from the second originating IP address;

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and success of said attempting a third communicable coupling is interpreted as a possibility including the detection; and

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and failure of said attempting a third communicable coupling is interpreted as a possibility including:

a network connectivity problem between the first tester and the system under test; and

the detection.

83. (Original) The network security testing method of claim 80, further comprising:

attempting a third communicable coupling by a second tester to the system under test;

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and success of said attempting a third communicable coupling is interpreted as a possibility including the detection; and

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and failure of said attempting a third communicable coupling is interpreted as a possibility including a network connectivity problem between the first tester and the system under test.

84. (Previously Presented) A computer program product for network security testing stored in a computer-readable medium, comprising:

instructions for attempting a first communicable coupling by a first tester for performing network security vulnerability testing to a network system under test;

instructions for executing a test to obtain network security vulnerability information by the first tester, wherein the test is targeted at the network system under test;

instructions for attempting a second communicable coupling by the first tester to the network system under test after executing the test to obtain network security vulnerability information; and

instructions for interpreting the combination success of the first communicable coupling and failure of the second communicable coupling as detection of the test by the network system under test.

85. (Canceled)

86. (Original) The computer program product of claim 84, further comprising:

instructions for attempting a third communicable coupling to the system under test;

wherein the attempting a first communicable coupling is made using a first originating IP address;

wherein the attempting a second communicable coupling is made using a second originating IP address that is essentially the same as the first originating IP address;

wherein the attempting a third communicable coupling is made using a third originating IP address that is different from the second originating IP address;

wherein the combination of success of the attempting a first communicable coupling, failure of the attempting a second communicable coupling, and success of the attempting a third communicable coupling is interpreted as a possibility including the detection; and

wherein the combination of success of the attempting a first communicable coupling, failure of the attempting a second communicable coupling, and failure of the attempting a third communicable coupling is interpreted as a possibility including:

a network connectivity problem between the first tester and the system under test; and

the detection.

87. (Original) The computer program product of claim 84, further comprising:

instructions for attempting a third communicable coupling by a second tester to the system under test;

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and success of said attempting a third communicable coupling is interpreted as a possibility including the detection; and

wherein the combination of success of said attempting a first communicable coupling, failure of said attempting a second communicable coupling, and failure of said attempting a third communicable coupling is interpreted as a possibility including a network connectivity problem between the first tester and the system under test.

88. (Previously Presented) A network security testing apparatus comprising:

a tester communicably coupled to a system under test for testing for network security vulnerabilities of a network system under test;

a test tool within the tester for performing a test to obtain specific network security vulnerability information for the network system under test, said test tool selectable responsive to adapt to the security obstacles of the network system under test detected based on information gained from a previous received information on network security vulnerability information;

an application programming interface (API) adapted to interface between said tester and said test tool, said API further including an API stub enabling said test tool to be executed by said tester even if the outputs of said tester do not directly correspond to the inputs of said test tool, and such that said test tool may be executed by said tester even if the inputs of said tester do not directly correspond to the outputs of said test tool, said API further including a common API for interfacing between the test tool and instructions provided to the test tool; and

wherein said tester is adapted to test the system under test by execution of said test tool.

89. (Original) A network security testing method comprising:

adapting an application programming interface (API) to interface between a tester and a test tool, such that the test tool may be executed by the tester even if the outputs of the tester do not directly correspond to the inputs of the test tool, and such that the test tool may be executed by the tester even if the inputs of the tester do not directly correspond to the outputs of the test tool;

executing the test tool by the tester;

wherein the test tool is targeted at a system under test; and

wherein the tester is communicably coupled to the system under test.

90. (Original) A computer program product for network security testing stored in a computer-readable medium, comprising:

instructions for adapting an application programming interface (API to interface between a tester and a test tool, such that the test tool may be executed by the tester even if the

outputs of the tester do not directly correspond to the inputs of the test tool, and such that the test tool may be executed by the tester even if the inputs of the tester do not directly correspond to the outputs of the test tool;

instructions for executing the test tool by the tester;

wherein the test tool is targeted at a system under test; and

wherein the tester is communicably coupled to the system under test.

91. (Canceled)

92. (Canceled)

93. (Canceled)

94. (Canceled)

95. (Canceled)

96. (Canceled)

97. (Canceled)

98. (Canceled)

99. (Canceled)

100. (Canceled)

101. (Canceled)

102. (Canceled)

103. (Previously Presented) A network security testing apparatus comprising:

a plurality of testers;

wherein each of said plurality of testers is adapted to communicably couple to a system under test;

wherein each tester of said plurality of testers has at least one quality of communicable coupling to the system under test, the at least one quality of communicable coupling including cost per bit, absolute speed, and geographical proximity of the selected tester to the system under test;

wherein a test of the system under test is performed by a selected tester of said plurality of testers, the selected tester being selected from said plurality of testers based at least partially upon said customer profile; and

wherein the selected tester is selected from said plurality of testers based at least partially on the selected tester's quality of communicable coupling.

104. (Previously Presented) A network security testing method comprising:

selecting a selected tester from a plurality of testers based at least partially on a tester's quality of communicable coupling, the quality of communicable coupling including at least one of cost per bit, absolute speed, and geographical proximity of the selected tester to the system under test; and

executing a test by the selected tester, wherein the test is targeted at a system under test, and wherein the selected tester is communicably coupled to the system under test.

105. (Previously Presented) A computer program product for network security testing stored in a computer readable medium, comprising:

instructions for selecting a selected tester from a plurality of testers based at least partially on a tester's quality of communicable coupling, the quality of communicable coupling including at least one of cost per bit, absolute speed, and geographical proximity of the selected tester to the system under test; and

instructions for executing a test by the selected tester, wherein the test is targeted at a system under test, wherein the selected tester is communicably coupled to the system under test.

106. (Canceled)

107. (Canceled)

108. (Canceled)

109. (Canceled)

110. (Canceled)

111. (Canceled)

EVIDENCE APPENDIX

U.S. Patent No. 6,301,668 to Gleichauf et al. ("Gleichauf I"), found beginning in paragraph 6 of the First Office Action (dated August 24, 2005), and found beginning in paragraph 2 of the Final Office Action (dated January 23, 2006);

U.S. Patent No. 6,324,656 to Gleichauf et al. ("Gleichauf II"), found beginning in paragraph 6 of the First Office Action (dated August 24, 2005), and found beginning in paragraph 2 of the Final Office Action (dated January 23, 2006);

Polk, "Automated Tools for Testing Computer Systems Vulnerability", http://www.nsi.org/Library/Compsec/CSECTOOL.txt, found beginning page 2 of the Final Office Action (dated January 23, 2006);

Li et al., "Effective load sharing on heterogeneous networks of workstations", Proceedings of 2000 International Parallel and Distributed processing Symposium, (IPDPS '00), May 2000, pp. 431-438, found beginning on page 12 of the Final Office Action (dated January 23, 2006); and

Srinivasan, "Binding Protocols for ONC RPC Version 2", Network Working Group RFC 1833, August 1995, found beginning on page 9 of the Final Office Action (dated January 23, 2006)

RELATED PROCEEDINGS APPENDIX

None.